

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

The contents of the Dropbox account associated with email
address arturo.rig.nava@gmail.com and User ID number
3177415152, that is stored at premises controlled by
Dropbox, Inc. located at 1800 Owens St Ste. 200, San
Francisco, CA

Case No. 2:23-mj-240

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the _____ Northern _____ District of _____ California _____, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251	Advertising for/of child pornography, in interstate commerce
18 U.S.C. §§ 2252 & 2252A	Receipt, distribution and/or possession of child pornography/visual depictions of minors engaged in sexually explicit conduct via a means or facility of interstate co

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Matthew W. Guinn

Applicant's signature

Matthew Guinn, Special Agent FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: April 11, 2023

City and state: Columbus, Ohio

Kimberly A. Johnson

United States Magistrate Judge



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**IN THE MATTER OF
THE SEARCH OF:**

The Dropbox account associated with the email address arturo.rig.nava@gmail.com and User ID number 3177415152, and information, that is stored at premises controlled by Dropbox, Inc. located at 333 Brannan St., San Francisco, CA 94107

Case. No. 2:23-mj-240

Magistrate Judge:

UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Matthew W. Guinn, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a SA with the FBI and have been since April 2012. I am currently assigned to the Child Exploitation and Human Trafficking Task Force Crimes Against Children Squad, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.
2. During my career as a SA, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses involving children. As part of my duties as a SA, I investigate criminal violations relating to child exploitation and child pornography, including the online enticement of minors and the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422.
3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts I believe to be necessary to establish probable cause for a search warrant for the content of the Dropbox Account associated with the email address arturo.rig.nava@gmail.com, User ID 3177415152 (hereinafter the “**SUBJECT ACCOUNT**”). I have not withheld any evidence or information which would negate probable cause.
5. The **SUBJECT ACCOUNT** to be searched is particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A – the production or attempted production, distribution, transmission, receipt, and/or possession of child pornography.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction

has been mailed, shipped or transported in or affecting interstate or foreign commerce.

This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

8. Title 18, United States Code, Section 2252A(a)(2), makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
9. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
10. The term "sexually explicit conduct," as used in 18 U.S.C. Section 2252, is defined pursuant to Title 18, United States Code, Section 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to Title 18, United States Code, Section 2256(2)(B), “sexually explicit conduct” when used to define the term child pornography, also means “(i) graphic

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.”

11. The term “minor,” as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
12. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”
13. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
14. The term “computer” is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
15. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
16. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are

in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

17. “Internet Protocol address” (IP address), as used herein, is a code consisting of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND MOBILE APPLICATIONS

18. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files (“objects”) may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
19. Computers, mobile computing devices (smart phones, tablets, and electronic storage media, hereinafter referred to as “mobile devices” or “mobile computing devices”) and computer technology have revolutionized the way in which child pornography is produced, utilized, and distributed. It has also revolutionized the way in which child pornography collectors interact with each other. Computers, mobile devices, and the Internet have facilitated the myriad ways in which child pornography is produced, stored, and distributed.
20. Nearly all mobile devices and many computers have the ability to take still and moving images. Such digital images and videos are easily stored, manipulated or transferred between devices using software or applications installed on each device. The capabilities of mobile devices, computers, electronic storage devices, and various internet technologies make the transfer and storage of and communication about such images and videos technically easy and inexpensive. Because of the proliferation of commercial services that

provide electronic mail service, chat services, and easy access to the internet, computers, mobile devices and the internet are the preferred method of distribution of child pornographic materials.

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol (“IP”) addresses² and other information both in computer data format and in written record format.
22. A growing and increasingly used phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as “apps,” are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such “apps” include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram.
23. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user’s true identity.

Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

24. Individuals can also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Gmail, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or mobile device capable of accessing the Internet. Apps related to this cloud-storage accounts can also be downloaded to a computer or mobile device, allowing easier access to the content of the accounts.

V. BACKGROUND REGARDING DROPBOX

25. Founded in 2007, Dropbox is a privately held electronic file storage service provider headquartered in San Francisco, California. Dropbox uses cloud computing to enable users to store and share files and folders with other users across the Internet using file synchronization. Dropbox provides both free and fee-based file sharing and file synchronization services. Dropbox conducts business throughout the United States and the world through its cloud-computing based file sharing services.
26. Dropbox offers a client application to facilitate the file synchronization and access on a wide variety of operating systems and devices owned or used by the account holder. Dropbox allows a user to create a Dropbox account, which is identified by the user's e-mail address and is secured with a user password. The e-mail address is the unique identifier for a Dropbox account. Once an account is created with Dropbox, the user must enter his or her e-mail address for the account, along with a valid user-created password in the login screen, in order to access the account. Since Dropbox accounts are not publicized and the general login screen does not show other valid e-mail accounts, the user must know the e-mail address in the first step to access a Dropbox account.
27. According to Dropbox's privacy policy, available at <https://www.dropbox.com/privacy>, Dropbox collects and stores "the files you upload, download, or access with the Dropbox

Service,” and also automatically maintains log data related to “information from your Device, its software, and your activity using the Services. This may include the Device’s Internet Protocol (“IP”) address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.” Dropbox describes itself as “a home for all your photos, docs, videos and files. Anything you add to Dropbox will automatically show up on all your computers, phones and even the Dropbox website – so you can access your stuff from anywhere.” See <https://www.dropbox.com/tour#!/tour/1>

28. In general, providers like Dropbox ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP address used to register the account and the IP addresses associated with the times a particular user has logged into the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.
29. In some cases, Dropbox account users will communicate directly with the provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.
30. In my training and experience, evidence of who was using a DropBox account and from where, and evidence related to criminal activity of the kind described above, may be found

in the files and records described above that are maintained by Dropbox. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

31. For example, the stored communications and media files connected to a DropBox account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, emails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.
32. In addition, the user’s account activity, logs, stored electronic communications and other data retained by Dropbox can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.
33. Therefore, Dropbox’s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Dropbox’s services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account’s user or users.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VII. INVESTIGATION AND PROBABLE CAUSE

35. On March 2, 2023, a Special Agent with the Child Exploitation Operational Unit in Washington, D.C. received information regarding seven videos depicting child sex abuse material (CSAM) involving a prepubescent female, approximately nine to ten years of age, and an adult male. The videos were observed on a TOR website and had been uploaded that day by a user utilizing the screen name “pogovka.” TOR is a free and open-source software for enabling anonymous communications and protects personal privacy by concealing a user’s location and usage from anyone performing network surveillance or traffic analysis. The thread on TOR was titled “Mexican father and his 12 year old daughter – NEW.” The seven videos depicted the child performing oral sex on the male as well as the male penetrating the child digitally and with his penis.
36. The agent was able to search an open-source image repository to locate an individual that was visually similar to the adult male in the videos. This subject was tentatively identified at that time as Arturo Navarrete-Juarez, residing at 2105 Gaylord Place, Columbus, OH 43232.
37. Additional open-source searches for Juarez yielded an Instagram account with the username inked.outsmoke and screen name of Arturo N. The account contains several photos of Juarez along with a photo posted on January 24, 2018, depicting an adult female with two prepubescent females and a baby. Juarez captioned the photo “Mi razon de ser” which translates to “My reason to be.”
38. Another photo in the Instagram account shows a close up of Juarez’s right hand, with very distinctive tattoos with various identifiable symbols and markings. A comparison of the tattoos on one of the subject’s hands in the seven videos of CSAM and the tattoos of Juarez on his Instagram account was done. Several of the distinct symbols on the hand of

the subject depicted in the videos are identical to the ones on Juarez's hand.

39. On December 15, 2022, officers with the Columbus Police Department (CPD) encountered Juarez. This interaction was captured on the body camera belonging to one of the officers speaking with Juarez. Juarez's face is clearly visible in the body camera video and closely resembles the face of the adult male in the CSAM videos.
40. On March 2, 2023, an emergency disclosure request was served on Meta Platforms, Inc. requesting account information for Instagram account inked.outsmoke. Meta Platforms responded with subscriber records for the account and a linked Facebook account with the user ID of arturo.navarrete.33234. Below is the response from Meta Platforms.
- | | |
|---------------------|-------------------------|
| Service: | Instagram |
| Account Identifier: | inked.outsmoke |
| Name First: | Arturo N. |
| Registered E-mail: | sicksmokemind@gmail.com |
| Vanity Name: | inked.outsmoke |
| Service: | Facebook |
| Account Identified: | 100024048422975 |
| Name: | Arturo Navarrete |
| Registered Email: | sicksmokemind@gmail.com |
41. An incident report taken by the Columbus Police Department ("CPD") on August 24, 2015, indicated that Juarez was involved in a weapons violation on that date involving another male subject. At that time, Juarez was located sitting in a vehicle with a female identified as Brooke L. Hernandez. Juarez advised officers at the time that Hernandez was his girlfriend and currently pregnant.
42. A search for Juarez through additional databases revealed that Brooke L. Hernandez is listed as an associate of Juarez. Hernandez has a reported current address of 2194 Muirwood Drive, Columbus, OH 43232 and her Ohio driver's license is registered at the same address. A comparison of Hernandez's driver's license photos indicates that she is the same woman with the minor children in the photos described above posted to Juarez's Instagram account.
43. 2194 Muirwood Drive is an apartment in the Chatham Village Apartment complex. A search of the Chatham Village website provided floor plans and photos of the various apartment options. A comparison of the photos provided on the website depicting the

interior of the available units and the interior location where the seven videos of CSAM were produced appear to be the same layout. In the website photos, an open set of stairs with white spindles and white trim leads from the first to the second floor between the living room and kitchen. A staircase similar in color and design is seen in the same location in the videos. In addition, there is a closet door underneath the staircase between the living room and kitchen which appears in both the website photos and videos. Lastly, the kitchen appears to be the same in both the photos and videos to include the location of the dishwasher, refrigerator and center island.

44. On March 9, 2023, a subpoena was served on Columbus City Schools requesting information regarding any students who are currently residing or have resided at 2194 Muirfield Drive in the last twelve months. Columbus City Schools responded with three juveniles that were associated with that address during the requested time frame. One of these juveniles is a female, hereinafter referred to as Jane Doe, with a date of birth of December 28, 2011. Further information revealed that Jane Doe was listed as residing at 2194 Muirwood Drive, Columbus, OH 43232 from October 12, 2021 to December 12, 2022. The parents for Jane Doe are listed as Brooke Hernandez and Juarez.
45. In addition, the minor's face is depicted several times in the various CSAM videos. The information received from Columbus City Schools also provided a current school photograph of Jane Doe. Jane Doe's school photo closely resembles the victim in the videos, both in age and facial features.
46. On March 13, 2023, Jane Doe was interviewed by an FBI Child and Adolescent Forensic Interviewer (CAFI). During that interview, Jane Doe reported she realized the police had come to her house for her dad, who is not her father, named Arturo. She disclosed that she had been raped by her father and the first time took place when she was around six years old. She reported he had his phone in his hand one time and she believed he was recording one time when he was rubbing his private part on her private part. The last time it happened she was ten years old. Jane Doe was able to identify herself, Juarez and background details from the recovered videos.
47. On March 9, 2023, affiant interviewed the property manager of 2194 Muirwood Dr., Columbus, OH. The property manager provided the following information: Arturo Navarrete-Juarez is not the current tenant at 2194 Muirwood Dr., Columbus, OH. His move-in date was August 13, 2021, and his move-out date was August 12, 2022. The e-

mail Juarez had provided was arturo.rig.nava@gmail.com and his phone number was 614-735-6107.

48. On March 10, 2023, the FBI conducted a search of the premises at 2105 Gaylord Place, Columbus, OH, pursuant to a federal search warrant. Juarez was also arrested at that time. Agents also interviewed Brooke L. Hernandez, mother of Jane Doe and mother of two of Juarez's children. During that interview, the interviewing agents showed Hernandez images taken from the CSAM video and Hernandez identified the individuals as Juarez and Jane Doe, and she identified furniture and articles of clothing.
49. On or about March 10, 2023, using open-source online checks, your affiant discovered that a Dropbox account was associated with email address Arturo.rig.nava@gmail.com. On March 15, 2023, your affiant served a subpoena on DropBox requesting subscriber information for that account. In response, DropBox provided the following subscriber records:

User ID: 3177415152

Full Name: arturo navarrete

Email Address: arturo.rig.nava@gmail.com

Account Creation Date: 2020-05-10 10:37:50 UTC

Account Status: Active

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

50. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved seeking/soliciting, receiving, distributing, and/or collecting child pornography:

- A. Those who seek out, exchange and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
- B. Those who seek out, trade and/or collect child pornography may collect sexually

explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- C. Those who seek out, trade and/or collect child pornography sometimes maintain hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- D. Those who seek out, trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- E. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

51. Based upon the conduct of individuals involved in seeking/soliciting, receiving,

distributing, and/or collecting child pornography set forth in the above paragraphs, and the facts learned during the investigation in this case, namely, that your affiant has reason to believe that the individual utilizing **SUBJECT ACCOUNT** has a sexual interest in minors and has viewed or distributed visual depictions of minors engaged in sexually explicit conduct utilizing an internet-capable device.

52. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of production, distribution and possession of child pornography is currently located within the **SUBJECT ACCOUNT**.

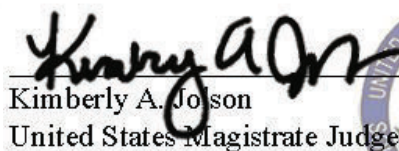
IX. CONCLUSION

53. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).
54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



Matthew W. Guinn
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 11th day of April, 2023.



Kimberly A. Johnson
United States Magistrate Judge



ATTACHMENT A

DESCRIPTION OF PLACE TO BE SEARCHED

This warrant applies to information associated with the Dropbox account that is associated with email address: arturo.rig.nava@gmail.com and User ID number 3177415152, which is stored at premises owned, maintained, controlled, or operated by Dropbox Inc., a company headquartered at 185 Berry Street, Suite 400, San Francisco, CA 94107.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

I. Information to be disclosed by Dropbox, Inc.

1. To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, Inc., including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Dropbox, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:
 - A. All records or other information regarding the identification of the user of the Subject Account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
 - B. All information automatically recorded by Dropbox Inc. from a user's device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Dropbox website, all information searched for on the Dropbox website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;
 - C. The types of service utilized by the user;
 - D. All records or other information stored by an individual using the account, including all files uploaded, downloaded or accessed using the Dropbox service, including all available metadata concerning these files and the dates and times they were uploaded to the account;
 - E. All records pertaining to communications between Dropbox Inc. and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations 18 U.S.C. §§ 2251, 2252 and 2252A, involving the use of a computer in or affecting interstate commerce to transport, receive, distribute, possess and/or access visual depictions of minors engaged in sexually explicit activity and/or child pornography including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to the following matters:
 - A. Any individuals' access to and interaction with minors.
 - B. All images depicting child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct.
 - C. All images, messages and communications between individuals relating to the above, including any and all preparatory steps taken in furtherance of these crimes.
 - D. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.